Dr. Varró Dániel bírálói kérdéseire adott válaszok

MTA doktori értekezés szerzője, címe:
Buttyán Levente
Új biztonsági mechanizmusok vezeték nélküli ad hoc és szenzorhálózatokban

Ezúton szeretném hálásan megköszönni Dr. Varró Dánielnek, hogy időt és energiát szánt MTA doktori értekezésem alapos átolvasására és megfogalmazta opponensi véleményét. Köszönöm az értekezéssel kapcsolatos észrevételeit és kérdéseit, melyeket az alábbiakban válaszolok meg:

1. Az 1. fejezetben a valós modellek (real-world model) matematikailag precíz leírására egy együttműködő Turing gépekre alapuló alacsonyszintű formális modell kerül bevezetésre. Mi a bevezetett formális modell előnye és hátránya más, a kommunikációs protokollok vizsgálatára elterjedten használt formális modellekhez képest? (pl. LTS: Labelled Transition Systems, CSP: Communicating Sequential Processes vagy egyéb processzalgebrák)

A kommunikációs protokollok vizsgálatára javasolt formális modellek (pl. LTS, CSP) hátránya a protokollok biztonsággal kapcsolatos tulajdonságainak vizsgálata esetén, hogy ezekben a modellekben explicit módon le kell írni a támadó viselkedését ahhoz, hogy a modell teljes legyen és a modellezett protokoll biztonsági tulajdonságait vizsgálni lehessen benne. A támadó explicit leírása azonban nem egyszerű, illetve minden ilyen leírásban benne van az a kockázat, hogy a modellezést végző valamit kifelejtett, és így a támadó modellje nem jól reprezentálja a valóságot. Különösen nehéz leírni a támadó által végrehajtható támadásokat, hiszen a modellt alkotó nem biztos, hogy minden lehetséges támadási módszert, technikát ismer.

A disszertációban alkalmazott modell előnye, hogy abban a támadó teljes viselkedését nem kell explicit módon leírni. A támadót reprezentáló automatákra (Turing gépekre) tettem ugyan néhány megkötést a vezeték nélküli kommunikációs képességeik tekintetében, de az általuk megvalósított támadásokat nem korlátoztam:

"While its communication capabilities are similar to that of the non-adversarial machines, Aj may not follow the routing protocol faithfully. In fact, we place no restrictions on the operation of Aj apart from being polynomial-time in the security parameter (e.g., the key size of the cryptographic primitives used in the protocol) and in the size of the network (i.e., the number of vertices). This allows us to consider arbitrary attacks during the analysis."

Tehát csupán annyit tettem fel, hogy a támadót reprezentáló automata polinom idejű algoritmust valósít meg, de hogy pontosan mit, azt nem adom meg, így a modell minden lehetséges praktikus támadást figyelembe vesz, és ilyen értelemben általános.

Ugyanakkor az alkalmazott modell hátránya, hogy a bizonyítások, a modellezett protokollok tulajdonságainak vizsgálata nehezen automatizálható, és így minden egyes protokoll biztonsági tulajdonságainak vizsgálata külön, "kézzel" végzett (manuális) elemzést, bizonyítást igényel (a disszertációban szereplő 1.1 tétel bizonyításához hasonlóan). Nagy vonalakban megadtam ugyan az ilyen bizonyítások javasolt gondolatmenetét, konkrét, automatizálásra alkalmas bizonyítási eljárást azonban nem tudtam javasolni. Megjegyzem ugyanakkor, hogy a javasolt hozzáállás (a modell finomításával) és a nagy vonalakban megadott bizonyítási módszer alkalmasnak bizonyultak más (sőt

más elvekre épülő) útvonalválasztó protokollok biztonságának hasonló elemzésére, lásd pl. az alábbi publikációkat:

- G. Ács, L. Buttyán, and I. Vajda, Provable security of on-demand distance vector routing in wireless ad hoc networks, Second European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS 2005), Visegrád, Hungary, July 13-14, 2005.
- G. Ács, L. Buttyán, and I. Vajda, The security proof of a link-state routing protocol for wireless sensor networks, IEEE Workshop on Wireless and Sensor Networks Security (WSNS 2007), Pisa, Italy, October 2007.
- G. Ács and L. Buttyán, Designing a secure label-switching routing protocol for wireless sensor networks, Periodica Polytechnica, Vol. 53, 2009.

Szeretném megjegyezni továbbá, hogy a disszertációban alkalmazott modell nem teljesen alkalmi, azt Pfitzmann, Backes, és Waidner, valamint Bellare, Canetti, és Krawczyk munkái inspirálták:

- M. Backes, B. Pfitzmann, Symmetric encryption in a simulatable Dolev-Yao style cryptographic library, 17th IEEE Computer Security Foundations Workshop, 2004.
- B. Pfitzmann and M. Waidner. A model for asynchronous reactive systems and its application to secure message transmission. In Proceedings of the IEEE Symposium on Research in Security and Privacy, May 2001.
- M. Bellare, R. Canetti, and H. Krawczyk. A modular approach to the design and analysis of authentication and key exchange protocols. In Proceedings of the ACM Symposium on the Theory of Computing, 1998.

Lényegében a fenti munkákban bevezetett szimuláció alapú modelleket adaptáltam ad hoc hálózati útvonalválasztó protokollok modellezésére.

2. A 2. fejezetben bevezetett kétszintű modell egy rendszermodellt és egy metamodellt foglal magában. A rendszermodell és metamodell viszonya azonban nem követi az objektumorientált programozás és modellvezérelt tervezés területén széleskörben használt metamodell és (példány)modell fogalmát, hanem inkább egy absztrakt és egy konkrét modell közötti viszonyt próbál szemléltetni. Mi a viszonya a disszertációban bevezetett kétszintű modellnek az (objektum-orientált) metamodell-modell viszonyhoz képest? Miként viszonyul a kétszintű modell a formális helyességellenőrzésben Galois-kapcsolatokon alapuló absztrakciós módszerekhez (pl. absztrakt interpretáció, predikátumabsztrakció)?

Az itt használt meta-modell fogalom nem azonos a modell-vezérelt szoftverfejlesztés területén használt meta-modell fogalommal. A modell-vezérelt szoftverfejlesztés területén a meta-modell és a modell között egy specifikus osztály-egyed reláció áll fenn, azaz a modell a meta-modell által definiált osztály egy példánya. Ilyen értelemben a modell tekinthető a meta-modell egy konkrét realizációjának vagy implementációjának. Az általam használt meta-modell kifejezés ennél általánosabb, és pusztán azt próbálja érzékeltetni, hogy egy modell modelljéről beszélünk, azaz konkrétan a játékelméleti modell (forwarding game) egy olyan modelljéről, melyben csak a csomópontok kooperációs szintjeinek alakulására fókuszálunk és elabsztraháljuk a játékelméleti modell minden más részletét (pl. a nyereségeket és költségeket). Mivel a disszertációmban egyáltalán nem jelennek meg szoftverfejlesztéssel kapcsolatos problémák és fogalmak, ezért ez a fogalom-választás talán elnézhető, bár kétségtelenül zavaró lehet olyan olvasók számára, akik a modell-vezérelt szoftverfejlesztés területén dolgoznak, és konkrét jelentést társítanak a meta-modell fogalomhoz.

Hasonlóan nincs köze a disszertációmban alkalmazott meta-modell absztrakciónak a számítógépes programok helyességellenőrzésénél használt absztrakt interpretáció fogalomhoz, ami a program-szemantika korrekt (sound) approximációjának elméletét jelenti, valamint a predikátum-absztrakció fogalomhoz, ami a konkrét programállapotok absztrakt állapotokkal történő leírását jelenti, ahol az absztrakció predikátumok egy halmazának a konkrét állapoton történő kiértékelésével valósul meg. Mégegyszer hangsúlyozom, hogy a disszertációm nem foglalkozik szoftverfejlesztésben használt modellekkel és program-elemzésben használt fogalmakkal és módszerekkel.

3. A 2.3-as altézishez kapcsolódóan a spontán kooperáció gyakoriságának felmérésére elvégzett véletlen szimuláción alapuló vizsgálatok (1. szimuláció) eredménye azt mutatta, hogy a kooperációt garantáló feltételek teljesülésének valószínűsége igen alacsony. Ez az eredmény azonban nem meglepő, hanem inkább az elvégzett véletlen szimulációk szükségszerű következménye. A függőségi hurok feltétele ugyanis értelmezhető egy strukturális (logikai) konzisztenciafeltételként gráfmodellek felett, amely globális feltételek esetén a gráfméret növelésével 1 valószínűséggel fog sérülni véletlen gráfok generálásakor (azaz, véletlenszerűen generált gráfmodell/hálózat aligha lesz konzisztens). Segítené-e a kooperáció biztonsági vizsgálatát olyan (konzisztens) gráfok automatikus generálása, amelyek garantáltan teljesítik az előírt strukturális feltételeket? (lásd pl. [1])

[1] O. Semeráth, A. Nagy, D. Varró. A graph solver for the automated generation of consistent domain-specific models. In Proc. of the 40th Int. Conf. on Software Engineering (ICSE '18), pp. 969–980. DOI: https://doi.org/10.1145/3180155.3180186

A disszertáció 2. fejezetében végzett szimulációs vizsgálatokban az ad hoc hálózatok témakörben megszokott módon generáltam a különböző szimulációs eseteket és állítottam be a szimuláció paramétereit. Alapvetően a hálózat topológiájára nem tettem megkötést, mert ez csak valamilyen konkrét alkalmazás feltételezése mellett lett volna lehetséges. Így egy adott 2 dimenziós területen egyenletes eloszlás szerint kerültek elhelyezésre a csomópontok egy teljesen általános, alkalmazás független esetet modellezve. Magát a topológia gráfot ezek után a csomópontok kommunikációs hatótávolsága (range) határozta meg. Az így nyert gráf nem véletlen gráf abban az értelemben, hogy csak az egymás kommunikációs hatótávolságában levő csomópontok lehetnek összekötve benne, és az ilyenek biztosan össze is vannak kötve. A randomitás tehát pusztán a csomópontok véletlenszerű elhelyezkedéséből adódik. Az ilyen gráfokat unit disk gráfoknak nevezik. Hasonlóan nem tettem megkötést arra vonatkozóan, hogy melyik csomópont melyik távoli csomóponttal kommunikálhat, hanem azt feltételeztem, hogy a csomópontok egyenletes eloszlás szerint bárkit választhatnak kommunikációs célcsomópontnak. Erre vonatkozóan szintén csak akkor lehetett volna megkötést tenni, ha valamilyen konkrét alkalmazást feltételeztem volna, melyből egy ilyen megkötés származhat. Miután a célcsomópont kiválasztásra került, a forrás és a cél között a legrövidebb utat választottam kommunikációs útvonalnak. Ez konzisztens a legtöbb ad hoc útvonalválasztó protokoll működésével, melyek igyekeznek a legrövidebb utat megtalálni két távoli csomópont között. Egy fenti módon generált szimulációs esetből direkt módon következik a csomópontok közötti függőségi reláció. A vizsgálat során, 1000 generált szimulációs esetből egy sem volt, melyben a spontán kooperáció kialakulását lehetővé tevő függőségek alakultak volna ki.

Nagyon fontos kiemelni, hogy a függőségi hurkok létezése nem strukturális konzisztencia-feltétel a modellben; semmi nem követeli meg ilyen hurkok létezését a valóságban, s így a modellben sem kell biztosítani a jelenlétüket. Ezért a vizsgált általános, alkalmazás független esetben az opponens által hivatkozott publikációban leírt módszert nem érzem alkalmazhatónak. Ugyanakkor, nagyon is elképzelhetőnek tartom, hogy ha valamilyen specifikusabb alkalmazási környezetet feltételezünk, mely megkötéseket ad a csomópontok elhelyezkedésére (pl. az nem egyenletes a síkon), a közeli csomópontok közötti kommunikációs linkek kialakulására (pl. rádiós jelterjedési viszonyok és különböző fizikai akadályok figyelembe vétele), a távoli csomópontok közötti kommunikációs

viszonyok kialakulására (pl. alkalmazás specifikus, hogy ki lehet forrás és ki lehet cél csomópont), illetve az útvonalválasztásra vonatkozóan (pl. konkrét útvonalválasztó protokollt feltételezünk), akkor az adott publikációban javasolt módszer alkalmazhatóvá válik és pontosabb szimulációs esetek előállítását teheti lehetővé.

Megjegyzem ugyanakkor, hogy nem tartom valószínűnek a spontán kooperáció feltételeinek kialakulását az ilyen alkalmazás specifikus esetekben sem, mégpedig azért, mert a függőségi hurkok kialakulása nagyban függ a kommunikációs útvonalaktól, ám a gyakorlatban az útvonalválasztó protokollok egyáltalán nem veszik figyelembe a hálózatban már meglevő függőségeket egy új útvonal választása esetén. Pl. tegyük fel, hogy egy már létező útvonalon A csomópont a forrás és B csomópont továbbító (forwarder) szerepet játszik (tehát A függ B-től). Ha most B szeretne valakivel kommunikálni, akkor egy A és B közötti közvetlen függőségi hurok kialakulásához olyan útvonalat kellene választania, ami átmegy A-n. De erre semmi garancia, hisz a létező útvonalválasztó protokollok nem a függőségek reciprocitására törekszenek, hanem kommunikációs szempontból optimális útvonalakat (pl. minél rövidebb utakat) választanak. Persze B függősége A-tól lehet közvetett is (azaz B függhet C-től, aki függhet D-től, ... aki függhet A-tól), de ez is teljesen esetleges, nincs arra garancia, hogy ilyen hosszabb függőségi hurkok mindig kialakulnak a hálózatban, ha amúgy az útvonalválasztás nem kifejezetten törekszik egy ilyen cél elérésére.

A függőségi hurkok létezése elengedhetetlen a kooperáció kialakulásához, hiszen ha egy csomópontnak nincs függőségi hurka, akkor a csomópont viselkedése (kooperációs szintje) nem befolyásolja a hálózat csomópont által tapasztalt viselkedését (throughput-ját). A disszertációban vizsgált modell statikus, és az eredményeim azt mutatják, hogy ez nem kedvez a kölcsönös függőségek kialakulásának. A statikus jelleg több dologból következik: a csomópontok nem mozognak (no mobility) és a modellben azt feltételeztem, hogy a választott kommunikációs viszonyok (forrás-célpont párok) sem változnak a szimuláció során, továbbá minden csomópont csak egy útvonalon játszik forrás szerepet. Azt sejthetjük, hogy egy kicsit dinamikusabb modellben, ahol a kommunikációs kapcsolatok és útvonalak az időben változnak, több esélye lenne a kölcsönös függőségek kialakulásának. Ezt a sejtést igazolja egy későbbi (follow-up) cikkünk, melyben Félegyházi Márk dinamikus változó, mobil ad hoc hálózatokban viszgálta a spontán kooperáció kialakulásának feltételeit:

- M. Félegyházi, J.-P. Hubaux, and L. Buttyán, Equilibrium Analysis of Packet Forwarding Strategies in Wireless Ad Hoc Networks -- the Dynamic Case, 2nd Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt 2004)m Cambridge, UK, March 24-26, 2004.

A fenti cikk fő konklúziója, hogy kooperatív Nash egyensúly sokkal nagyobb valószínűséggel alakul ki spontán módon, ha a hálózat nem statikus. Itt is szükség van azonban egy kis "nagylelkűségre", ami a pillanatnyi függőségi aszimmetriák kiegyensúlyozására szolgál. A cikkben azt mutattuk meg, hogy mikor minden csomópont ún. Generous TFT stratégiát játszik, akkor ez Nash egyensúlyhoz vezet a rendszerben, és az ehhez szükséges "nagylelkűség" mértéke a mobiltás mértékétől függ: minél dinamikusabban változik a hálózat, annál kisebb az a nagylelkűségi küszöb (generosity threshold), ami biztosítja, hogy a szimulációs esetek 95%-ában teljes kooperáció kialakulását figyeljük meg a hálózatban.

4. A 3. fejezetben elvégzett szimulációs vizsgálatok a hamis pozitív rátát (nincs féregjarat, de van hamis riasztás), valamint a helyes riasztások arányát (valós pozitív) mérik fel, nem egyértelmű azonban, hogy miként kerülhetők el a hamis negatív esetek (van féregjárat, de nincs riasztás), illetve ennek jelenlétében miként mérhető fel ezek aránya.

A hamis negatív ráta ebben az esetben a valós pozitív rátából számolható. A szimulációs vizsgálatokban pontosan egy féregjáratot helyeztem el véletlenszerűen a hálózatban és megmértem a *p* pozitív detekciós rátát. Ezt úgy tettem, hogy adott paraméter beállítások mellett 100 szimulációt futtattam, majd megszámoltam azon futások számát ahol az elhelyezett féregjáratot detektálta az algoritmus. Ebből következik, hogy a többi futásban nem detektálta, azaz a hamis negatív ráta 1-*p*.

5. Miként lenne elvégezhető a 3. fejezetben javasolt elosztott féregjárat-detekciós algoritmus releváns paramétereinek (pl. hamis pozitív ráta, stb.) kiértékelése?

A hamis pozitív döntés ebben az esetben azt jelenti, hogy a protokoll futása végén a felek számára úgy tűnik, hogy nem közvetlen szomszédok (azaz féregjáraton keresztül hallják egymás üzeneteit), miközben valójában közvetlen szomszédok. Ezt a támadó mindig el tudja érni a protokoll distance bounding fázisában átküldött üzenetek késleltetésével. A disszertációban is említettem, hogy a protokoll csak egy felső becslést ad a felek távolságára, azaz a valódi távolság mindig lehet kisebb, mint a protokollban becsült távolság. Ezzel a támadó meg tudja akadályozni, hogy közvetlen fizikai szomszédok egymással logikai szomszéd kapcsolatot alakítsanak ki, és ha ezt sok szomszédos pár között eléri a támadó, akkor modhantjuk, hogy egyfajta Denial-of-Service helyzetet idézett elő. Ez azonban tipikusan nem célja egy féregjáratot használó támadónak, hiszen ő éppen ellenkezőleg, azt szeretné elérni, hogy akik nem közvetlen fizikai szomszédok azok mégis annak érzékeljék egymást.

A hamis negatív döntés azt jelenti, hogy a protokoll futása végén a felek közvetlen szomszédnak gondolják magukat, miközben valójában távol vannak egymástól (azaz féregjáraton keresztül hallják egymást, de ezt nem veszik észre). Ez az igazán érdekes eset, és ennek valószínűségére vonatkozik az opponensi kérdés. Mivel a felek a protokoll harmadik fázisában hitelesítik a küldött és kapott (r_i és s_i) biteket, ezért a támadó vagy úgy érheti el célját, hogy a bitek hitelesítését meghamisítja, vagy pontosan előre ismeri a felek bitjeit és előbb tudja elküldeni a felek üzeneteit a distance bounding fázisban, mint ahogy azt maguk a felek kiküldik. A hitelesítés meghamisítása a MAC függvény tulajdonságai miatt (egyirányúság és megfelelően nagy kimenet méret) gyakorlatilag lehetetlen (elenyésző valószínűségű). A biteket a commitment fázisban átküldött hash értékekből próbálhatja meg kitalálni a támadó, ez azonban az alkalmazott kriptográfiai hash függvény egyirányúsága (ősképellenállósága) miatt gyakorlatilag lehetetlen (elenyésző valószínűségű). Így csak a bitek tippelése marad a támadó számára, mint lehetőség, és így annak valószínűsége, hogy minden bitet helyesen eltalál 2^(-2l), ami l megfelelő megválasztásával tetszőlegesen kicsivé tehető (annak árán, hogy sok üzenetváltásra van szükség a protokollban). Összességében tehát, ha az alkalmazott MAC és hash függvények biztonságosak, akkor az l biztonsági paramétertől függ a támadás sikere, és l megfelelően nagy értékre állításával tetszőlegesen kicsivé tehető.

A protokoll azonban még ennél is többet nyújt, mert azt is biztosítja, hogy még egy csalárd módon viselkedő protokoll résztvevő sem tudja magáról elhitetni egy becsületes másik féllel, hogy közelebb van hozzá, mint valójában. Tegyük fel pl. hogy x becsületes, de y csalni próbál. y egyik lehetősége, hogy megsejti x r_i bitjeit, és már az x-től érkező üzenetek vétele előtt elküldi válaszait x-nek a distance bounding fázisban. A fentiekhez hasonlóan, annak valószínűsége, hogy ezt minden l bitre sikeresen meg tudja tenni 2^(-l), ami l megfelelő megválasztásával tetszőlegesen kicsivé tehető. y másik lehetősége, hogy az előre küldött üzeneteinek megfelelő biteket hitelesít a protokoll harmadik fázisában. Ezt hivatott kivédeni a commitment fázis, ahol y-nak még a distance bounding fázis előtt el kell köteleznie magát a bitjei mellett. A commitment biztosítja, hogy ezeket a biteket később már nem

tudja megváltoztatni, míg a commitment felnyitásáig (ami a harmadik fázisban történik az r' és s' átküldésével) x nem tudja mik ezek a bitek. Összességében tehát még egy olyan résztvevő sem tudja magát közelebb hazudni a másik félhez, aki csalni próbál és nem követi hűen a protokollt.

6. Az 5. fejezet privacy-megőrző partnerhitelesítést egy limitált erőforrásokkal rendelkező környezetben vizsgálja, ugyanakkor nem világos, hogy pontosan milyen erőforrás feltételek teljesülése esetén lesznek érvényesek a javasolt eredmények.

Az alapvető feltevés ebben a fejezetben az volt, hogy a hitelesített eszközök olyan erőforrás korlátokkal rendelkeznek, ami nem teszi lehetővé publikus kulcsú kriptográfia használatát rajtuk. Ebből fakadt a fejezetben vizsgált probléma, miszerint ha csak szimmetrikus kulcsú kriptográfiai primitívek használhatók, akkor az ellenőrző félnek tudnia kell, milyen kulccsal ellenőrizze a hitelesítő protokollban beérkező üzeneteket. Ehhez nem adhat segítséget a hitelesített eszköz, mert azzal a privacy sérül (azaz minden segítség a támadó számára is segítség annak kiderítéséhez, hogy ki hitelesíti éppen magát). Ha sok potenciális hitelesített eszköz van és az eszközök egyedi kulcsot használnak (ami azért előnyös, mert így egy eszköz kompromittálódása nem érint más eszközöket), akkor az ellenőrző félnek minden lehetséges kulcsot végig kell próbálgatnia, ami jelentős késleltetéshez vezethet. Az 5. fejezetben javasolt megoldás egy kompromisszumot valósít meg, melyben az ellenőrző félnek ugyan próbálgatnia kell bizonyos kulcsokat, de az ez által okozott késleltetés egy előre adott küszöb alatt marad, míg egyúttal a rendszer által nyújtott privacy mértéke a lehető legnagyobb.

A javasolt eredmények tehát minden olyan esetben érvényesek, mikor potenciálisan nagy számú eszköz hitelesítésére van szükség és az alkalmazási környezet nem teszi lehetővé publikus kulcsú kriptográfia használatát. Egy tipikus ilyen alkalmazás a gyakorlatban egy elektronikus jegyeket használó tömegközlekedési rendszer, melyben az elektronikus jegyek RFID vagy NFC technológiát használó kontaktus mentes chip kártyák. A jegyek/kártyák érvényesítése a kártyák hitelesítését igényli a kártya olvasó felé. Ezek a kártyák (pl. NXP Mifare Classic[1] vagy NXP Mifare Ultralight[2]) tipikusan nem képesek publikus kulcsú kriptográfiára (de ha képesek lennének, valószínűleg akkor sem ezt használnák a hitelesítéshez teljesítmény okok miatt). A hitelesítésnek egy adott időkorláton belül (pl. néhány tized másodperc) le kell zajlania a kártya és az olvasó között. A kártyák nyomonkövetése pedig (location) privacy problémákhoz vezet. Tehát minden olyan feltétel adott, amiből az 5. fejezetben kiindultam, így az ott javasolt privacy-megőrző hitelesítő eljárás egy ilyen alkalmazásban előnyösen alkalmazható (hatékony és segít elkerülni a felhasználók nyomonkövetését).

Budapest, 2021. március 12.

.....

Buttyán Levente

[1] https://www.nxp.com/docs/en/data-sheet/MF1S70YYX_V1.pdf

[2] https://www.nxp.com/docs/en/data-sheet/MF0ICU2.pdf